

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-101529

(P2003-101529A)

(43) 公開日 平成15年4月4日 (2003.4.4)

(51) Int.Cl. ⁷	識別記号	F I	テマート* (参考)
H 0 4 L 9/16		G 0 6 F 12/14	3 2 0 B 5 B 0 1 7
G 0 6 F 12/14	3 2 0	G 1 1 B 20/10	H 5 C 0 5 2
G 1 1 B 20/10		H 0 4 N 5/76	A 5 C 0 5 3
H 0 4 N 5/76			Z 5 C 0 6 3
		7/173	6 3 0 5 C 0 6 4

審査請求 有 請求項の数 8 O L (全 11 頁) 最終頁に続く

(21) 出願番号 特願2001-287374(P2001-287374)

(22) 出願日 平成13年9月20日 (2001.9.20)

(71) 出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 大喜多 秀紀

神奈川県横浜市磯子区新杉田町8番地 株

式会社東芝横浜事業所内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外6名)

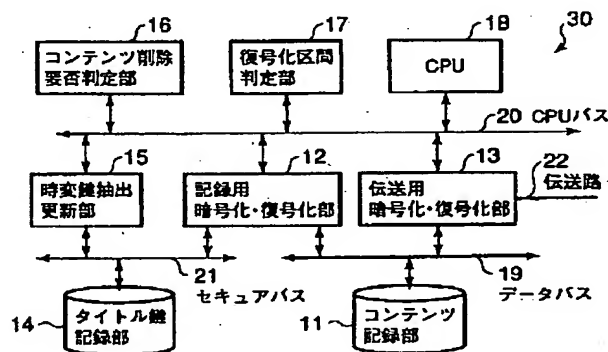
最終頁に続く

(54) 【発明の名称】 コンテンツ管理装置およびコンテンツ削除方法

(57) 【要約】

【課題】 著作権保護機能により保護されたコンテンツをMOVE処理もしくはPAUSE処理する際に、元のコンテンツを安全かつ効率的に削除する。

【解決手段】 タイトル鍵記録部14はコンテンツ暗号化・復号化のためのタイトル鍵を記録する。記録用復号化・暗号化部12はタイトル鍵記録部14に記録された鍵を用いてコンテンツを復号化する。時変鍵抽出更新部15はコンテンツ中の各ブロックを復号化する際生成された時変鍵を抽出する。又、時変鍵抽出更新部15はタイトル鍵記録部14が記録するタイトル鍵を、抽出された時変鍵で更新する。



【特許請求の範囲】

【請求項1】 コンテンツ暗号化・復号化のためのタイトル鍵を記録するタイトル鍵記録手段と、前記タイトル鍵記録手段に記録された鍵を用いて前記コンテンツをブロック単位に復号化する復号化手段と、前記復号化手段により前記コンテンツ中の各ブロックが復号化される際に生成される時変鍵を抽出する時変鍵抽出手段と、

前記タイトル鍵記録手段が記録するタイトル鍵を前記時変鍵抽出手段により抽出された時変鍵で更新する鍵更新手段、を有することを特徴とするコンテンツ管理装置。

【請求項2】 コンテンツに付加された著作権保護情報を基にコンテンツ削除の要否を判定するコンテンツ削除要否判定手段を更に具備し、前記鍵更新手段は、前記コンテンツ削除要否判定手段によりコンテンツ削除が必要と判断された場合、前記タイトル鍵記録手段に記録された鍵の更新を行うことを特徴とする請求項1に記載のコンテンツ管理装置。

【請求項3】 前記特定区間分のコンテンツ復号化が完了したかどうかを判定する復号化区間判定手段を更に具備し、前記鍵更新手段は該復号化区間判定手段により前記特定区間の復号化が完了したと判定された場合、前記タイトル鍵記録手段に記録された鍵の更新を行うことを特徴とする請求項1に記載のコンテンツ管理装置。

【請求項4】 前記復号化手段は、あるブロックの暗号化・復号化に用いる時変鍵として少なくとも2つ以上前のブロックの暗号化・復号化により得られた時変鍵を用いることを特徴とする請求項1に記載のコンテンツ管理装置。

【請求項5】 前記復号化手段は、前記特定区間の最後のブロックの復号化の際、前ブロックの最後の復号化により導出された時変鍵を用いることを特徴とする請求項4に記載のコンテンツ管理装置。

【請求項6】 コンテンツの暗号化・復号化のためのタイトル鍵をタイトル鍵記録領域に記録するステップと、タイトル鍵記録領域に記録された鍵を用いて前記コンテンツを復号化するステップと、コンテンツ復号化の際生成される時変鍵を抽出するステップと、

前記タイトル鍵記録領域に記録されたタイトル鍵を前記時変鍵で更新するステップ、を有するコンテンツ削除方法。

【請求項7】 コンテンツに付加された著作権保護情報を基にコンテンツ削除の要否を判定するステップと、前記コンテンツ削除が必要と判断された場合、前記タイトル鍵領域の更新を行うステップを有することを特徴とする請求項6に記載のコンテンツ削除方法。

【請求項8】 特定区間分のコンテンツ復号化が完了したかどうかを判定するステップと、前記特定区間の復号化が完了した場合、タイトル鍵領域

の更新を行うステップとを有することを特徴とする請求項6に記載のコンテンツ削除方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は放送局側から配信されたコンテンツに対してMOVE処理・PAUSE処理を行う場合のコンテンツ削除方法に関する。

【0002】

【従来の技術】 著作権保護機能により保護されたコンテンツをMOVE処理もしくはPAUSE処理する場合、著作権保護機能により定められたルールに従い、伝送もしくは記録後特定時間経過したコンテンツを装置から順次削除していく必要がある。

【0003】 MOVE処理は、Copy Onceコンテンツ（1回だけ記録を許されたコンテンツ）に対するコンテンツ移動処理である。Copy Onceコンテンツは記録が1回しか許可されていないため、他の記録媒体へのコピーは許可されていない。しかしコンテンツを例えば受信器の記録部に記録した後、該コンテンツの削除を条件に、他の記録先機器へ記録することが許されている。

【0004】 PAUSE処理は、Copy Neverコンテンツ（記録が許可されていないコンテンツ）に対するタイムシフト視聴処理である。タイムシフト視聴は、放送中のコンテンツに対して一時停止やプレイバック再生を行う機能であり、コンテンツ視聴時のコーヒープレイクやトイレ休憩（一時停止）やスポーツ中継などでの決定的瞬間のインスタントリプレイ（プレイバック再生）を提供できる。PAUSE処理ではコンテンツを一定時間後削除することを条件に、例えば受信器の記録部に記録することが許されている。

【0005】

【発明が解決しようとする課題】 MOVE処理もしくはPAUSE処理においてコンテンツを削除する方法として、従来以下のようないくつかの方式が考えられる。

【0006】 まず第1の方式として、コンテンツデータそのものを削除していく方式が考えられる。しかし一般にコンテンツは膨大なデータ量がある。例えば通常のVHS並みの画質の映像コンテンツの場合で約5Mbps（Mega bit per second）程度、ハイビジョン画質の映像コンテンツで約28Mbps程度のデータ量がある。このような大量データの削除をMOVE・PAUSE処理と同時に行うことは負荷の大きい処理であり現実的でない。

【0007】 第2の方式として、コンテンツそのものを削除する代わりに、記録されたコンテンツを復号化不可能とするため、コンテンツの復号化に用いるタイトル鍵を消去する方式が考えられる。しかし、通常コンテンツ1つに対してタイトル鍵は1つであり、例えばMOVE処理中の障害によるクラッシュ時に、コンテンツが送受

信側の双方に存在する、もしくは双方から消失するという事態が生じない様、コンテンツを送送し終えるまで、タイトル鍵の削除・伝送が行えない。

【0008】このため送信側ではコンテンツを送信分のみを削除することができず、受信側ではコンテンツをすべて受信するまで復号化ができないという問題が生じる。このような問題のためコンテンツが映像ストリームや音声ストリームの場合など、伝送中にコンテンツを復号化してリアルタイムで再生・伝送・消去する必要がある場合に、この方式は適用できない。

【0009】第3の方式として、コンテンツを複数の領域に分割し、それぞれを別のタイトル鍵で暗号化し、コンテンツの削除が必要になった場合、対応するタイトル鍵を順に削除していく方式が考えられる。当該方式はコンテンツが映像ストリームの場合に対しても有効であるが、コンテンツを細かく分割した場合、管理するタイトル鍵が膨大になるという問題がある。例えばコンテンツをフレーム単位に分割したとすると、1時間の映像コンテンツに対して10万以上のタイトル鍵を管理する必要が生じる。

【0010】タイトル鍵はコンテンツの著作権保護のため機密にする必要があり、通常のシステムからはアクセスできない保護領域で管理する必要がある。機密性を確保する必要のある保護領域を大量に準備することは現実的ではなく、当該方式によるコンテンツ削除をMOVE処理やPAUSE処理に対して適用することは事実上困難である。

【0011】本発明は上記の問題点に鑑み、著作権保護機能により保護されたコンテンツをMOVE処理もしくはPAUSE処理する際に、元のコンテンツを安全かつ効率的に消去することを目的としている。

【0012】

【課題を解決するための手段】上記目的を達成するために本発明は、コンテンツ暗号化・復号化のためのタイトル鍵を記録するタイトル鍵記録手段と、前記タイトル鍵記録手段に記録された鍵を用いて前記コンテンツをブロック単位に復号化する復号化手段と、前記復号化手段により前記コンテンツ中の各ブロックが復号化される際に生成される時変鍵を抽出する時変鍵抽出手段と、前記タイトル鍵記録手段が記録するタイトル鍵を前記時変鍵抽出手段により抽出された時変鍵で更新する鍵更新手段を有する。

【0013】これにより、HDD、DVDもしくはSDカードなどCPRMにおけるC-CBC暗号などを用いて復号化したコンテンツを復号化が完了したのから順に効率的に削除することができる。

【0014】更に本発明は、コンテンツに付加された著作権保護情報を基にコンテンツ削除の要否を判定するコンテンツ削除要否判定手段を具備し、前記鍵更新手段は、前記コンテンツ削除要否判定手段によりコンテンツ

削除が必要と判断された場合、前記タイトル鍵領域の更新を行う。これにより、コンテンツ削除処理を、MOVE処理・PAUSE処理などコンテンツ削除が必要な場合に適切に呼び出すことが出来る。

【0015】又本発明は、前記特定区間分のコンテンツ復号化が完了したかどうかを判定する復号化区間判定手段を更に具備し、前記鍵更新手段は特定区間の復号化が完了した場合、前記タイトル鍵領域の更新を行う。

【0016】これにより、タイトル鍵の更新（すなわちコンテンツの削除）を、IEEE1394パケット単位や、MPEG2のフレーム、GOP単位などまとまった単位で行うことが出来、必要以上に頻繁にタイトル鍵を更新することによる処理効率の低下を防ぐことが出来る。

【0017】又本発明は、あるブロックの暗号化・復号化に用いる時変鍵として、少なくとも2つ以上前のブロックの暗号化・復号化により得られた時変鍵を用いる。例えば、前記特定区間の最後のブロックの復号化の際、前ブロックの最後の復号化により導出された時変鍵を用いる。これにより、特殊再生やコンテンツのサーチを行う際、処理に必要な時変鍵を高速に生成が出来る。

【0018】

【発明の実施の形態】以下、図面を参照しながら本発明の実施の形態について詳細に説明する。図1は本発明に係るコンテンツ管理装置の構成の一実施形態を示すブロック図である。

【0019】本発明のコンテンツ管理装置30は、コンテンツ伝送を行うデータバス19、制御情報をやり取りするCPUバス20、タイトル鍵や時変鍵を安全にやり取りするセキュアバス21の3つのバスを用いて構成されている。

【0020】コンテンツ記録部11はコンテンツを記録あるいは一時蓄積する。記録用暗号化・復号化部12はコンテンツに付加された著作権保護情報に基づき、コンテンツの暗号化・復号化を行う。記録用暗号化・復号化の具体例としてはCPRM(Content Protection for Recordable Media)などがある。

【0021】コンテンツ記録部11に記録された情報は、記録用暗号化・復号化部12を通じて復号化され、データバス19を介して伝送用暗号化・復号化部13に転送される。伝送用暗号化・復号化部13では受け取ったコンテンツを伝送用に暗号化し伝送路22に流す。伝送路の具体例としてはIEEE(The Institute of Electrical and Electronics Engineers, Inc.)で規格化されているIEEE std. 1394-1995(IEEE1394)などがある。伝送用暗号化・復号化の具体例としては、DTCP(Digital Transmission Content Protecti

on) などがある。

【0022】記録用暗号化・復号化部12は、セキュアバス21を介してタイトル鍵記録部14からタイトル鍵情報を受け取り、当該タイトル鍵を用いてコンテンツの暗号化・復号化を行う。タイトル鍵記録部14は、不正アクセスを防ぐため通常の方法では読み出せない保護領域である。つまりタイトル鍵記録部14は、CPUバス20から直接アクセスすることはできず、記録用暗号化・復号化部12とタイトル鍵記録部14との認証処理を介してアクセス可能である。

【0023】コンテンツ削除要否判定部16はコンテンツに付与された著作権保護情報および現在の実行状態に基づきコンテンツ削除の要否を判定する。実行状態の具体例としてはMOVE処理中もしくはPAUSE処理中などがある。時変鍵抽出更新部15は、記録用暗号化・復号化部12から暗号化・復号化の際生成する時変鍵（後述される）を抽出し、コンテンツ削除要否判定部16の判定結果に応じて、コンテンツ削除の必要があればタイトル鍵記録部14のタイトル鍵を、抽出した時変鍵により更新する。復号化区間判定部17は特定区間の復号化が完了したかどうかを判定する。CPU18は本発明に従ってコンテンツ管理装置30を総合的に制御する。

【0024】図2はコンテンツに付与される著作権保護情報の一例を示す。「00」が付されたコンテンツはCopy Freeコンテンツであって、コピーを自由に行うことができる。「10」が付されたコンテンツはCopy Onceコンテンツであって、コピーが1度だけ許可されている。Copy Onceコンテンツを記録媒体にコピーした場合、該著作権保護情報は「01」に書き換えられ、以後のコピーが禁止される。「11」が付されたコンテンツはCopy Neverコンテンツであって、コピーは禁止されている。

【0025】図3は著作権保護のかかったコンテンツに対するMOVE・PAUSE処理の概要を示す図である。

【0026】PVR (Personal Video Recorder) 31はコンテンツ管理装置30を具備する装置の一具体例であり、HDDを内蔵しコンテンツを記録あるいは一時蓄積する機能を持つ。表示装置32はテレビジョンなどに代表される機器で、デジタルもしくはアナログ映像を画面に表示する機能を持つ。記録装置33はDVHSやAV-HDD、DVDなどに代表される機器で、映像の記録機能を持つ。PVR31は必要に応じてMOVE処理もしくはPAUSE処理を行う。

【0027】MOVE処理は、Copy Onceコンテンツに対するコンテンツ移動処理であるため、他の記録媒体へのコピー（ダビング）は許可されていない。しかしコンテンツをコンテンツ記録部11のような受信器

の記録媒体に記録した後、該コンテンツの削除を条件に、他の記録先機器へ移動することが許されている。MOVE処理は、このようなコンテンツ移動処理を示す。

【0028】MOVE処理では著作権保護に関する規定上、コンテンツの移動途中に障害が発生したとしても、送信元であるPVRと受信先である記録装置に同一コンテンツが重複して存在することのないよう適切に制御されなければならない。また、1台のPVR31の出力を複数台の記録機器で記録する操作は、コンテンツの複製を作成する操作となるためMOVE処理では許可されていない。

【0029】Copy Neverコンテンツは記録媒体への記録は許可されていないが、PAUSE処理では記録時間に制限を設けることにより、コンテンツ記録部11のような記録媒体への一時蓄積を許可し、一時停止やプレイバック再生を可能としている。制限時間の具体例としては、90分や1日あるいは1週間などがある。一時蓄積したコンテンツは制限時間経過後削除する必要がある。

【0030】PAUSE処理は、DTCP規格ではRETENSION処理とも呼ばれており、処理に関する名称は本発明の限りではない。また、PAUSE処理を、Copy Onceコンテンツに対して適用することも可能である。

【0031】図4は、MOVE処理を具体的に説明する図である。

【0032】コンテンツはIEEE1394などのセキュアな伝送路22を経由して、PVR31等の送信側機器から記録装置33等の受信側機器に伝送される。送信側機器では送信済みのコンテンツを適切な手段で削除する必要がある。

【0033】図5はPAUSE処理を具体的に説明する図である。

【0034】矩形は記録領域を模式的に表したものである。記録位置は記録領域を左から右へ移動し、記録位置の左側はコンテンツが記録されている領域を表す。再生位置は記録位置より左側の制限時間内で自由に移動させることが出来る。記録してから制限時間を超過したコンテンツ（例えば記録後90分経過したコンテンツ）は順次削除していく。

【0035】図6は従来におけるコンテンツを削除する第1の方式を示した図である。

【0036】当該方式では、コンテンツデータそのものを削除していく（例えば各データを「00」に書き換える）。しかし一般にコンテンツは膨大なデータ量がある。例えば通常のVHS並みの画質の映像コンテンツの場合で約5Mbps (Megabit per second) 程度、ハイビジョン画質の映像コンテンツで約28Mbps程度のデータ量がある。このような大量データの削除をMOVEあるいはPAUSE処理と同時に

行うことは負荷の大きい処理であり現実的でない。

【0037】図7は従来におけるコンテンツを削除する第2の方式を示した図である。

【0038】当該方式では、コンテンツそのものを削除する代わりに、コンテンツの復号化に用いるタイトル鍵を消去する。タイトル鍵を消去することにより、暗号化されたコンテンツを復号化することは不可能となり、結果的にコンテンツそのものを削除するのと同じ効果が得られる。タイトル鍵は通常54bitや128bitなどのサイズでありコンテンツそのものの削除と比較して処理も容易である。当該方式はコンテンツが暗号化ファイルの場合など、コンテンツをすべて転送してから復号化のための鍵を送付する処理方式に対して有効である。

【0039】しかし当該方式では、通常コンテンツ1つに対してタイトル鍵は1つであり、送信側ではコンテンツを送信し終えるまでタイトル鍵の削除が行えず、受信側ではコンテンツをすべて受信するまで復号化ができないという問題が生じる。このためコンテンツが映像ストリームや音声ストリームの場合など、伝送中にコンテンツを復号化してリアルタイムで削除する必要がある場合には適用できない。

【0040】図8は従来におけるコンテンツを削除する第3の方式を示した図である。

【0041】当該方式では、コンテンツを複数の領域に分割し、それぞれを別のタイトル鍵で暗号化する。そしてコンテンツの削除が必要になった場合、対応するタイトル鍵を順に削除していく方式をとる。当該方式はコンテンツが映像ストリームの場合に対しても有効であるが、コンテンツを細かく分割した場合、管理するタイトル鍵が膨大になるという問題がある。例えばコンテンツをフレーム単位に分割したとすると、1時間の映像コンテンツに対して10万以上のタイトル鍵を準備し管理する必要が生じる。タイトル鍵はコンテンツの著作権保護のため機密にする必要があり、通常のシステムからはアクセスできない保護領域で管理する必要がある。機密性を確保する必要がある保護領域を大量に準備することは現実的ではなく、当該方式によるコンテンツ削除をMOVE処理やPAUSE処理に対して適用することは事実上困難である。

【0042】図9は上記問題点を鑑みて発明されたものであり、本方式におけるコンテンツを削除する方式の概略を示した図である。本方式では、コンテンツ復号化の際使用される時変鍵を抽出し、タイトル鍵領域の元のタイトル鍵を、抽出した当該時変鍵で順次上書きする方式をとる。これにより更新した時変鍵より前のコンテンツの復号化を不可能とする。

【0043】図10はコンテンツ暗号化方式の一例を示す。ここでは暗号化方式としてC-CBC(Converted Cipher Block Chaining)を用いた暗号化処理について示す。C-CBCでコ

ンテンツを暗号化する際、暗号化に用いる暗号鍵の推定を困難にし暗号強度を高めるため、処理途中で暗号鍵を変更する時変鍵方式という処理方式を用いる。ここで暗号鍵はタイトル鍵と同義である。この時変鍵は元の暗号鍵と平文コンテンツから計算により求めることができる。計算には逆演算の困難な一方方向性関数を用いる。これにより暗号化コンテンツから平文コンテンツや暗号鍵を推定することを困難とし暗号強度を高めている。

【0044】図10では、コンテンツをブロック単位に分割した上で、まずタイトル鍵と最初のブロックを暗号化する。この暗号化の際導出された時変鍵を用いて第2のブロックを暗号化する。以下当該処理を各ブロックに順次適用することでコンテンツを暗号化する。

【0045】図11は図10で示した暗号化方式により、暗号化されたコンテンツを復号化する処理を示した図である。この復号化処理は、図10で説明した暗号化処理とは逆の手順となり、タイトル鍵もしくはその時変鍵と暗号化コンテンツから平文コンテンツへの復号化を順次行っていく。

【0046】以下、本発明におけるMOVE・PAUSE処理におけるコンテンツ削除方法について詳細に示す。

【0047】図12は本発明に係るコンテンツ復号化の際に行われるコンテンツ削除処理の第1の実施形態について示した図である。本方式では、コンテンツ復号化の際導出された時変鍵を抽出し、抽出された時変鍵で元のタイトル鍵を更新する処理を追加したことに特徴がある。

【0048】記録用暗号化・復号化部12は先ずブロックB1をタイトル鍵を用いて復号化する。このタイトル鍵はPVR31が各コンテンツ毎に予め持っている値であり、タイトル鍵記録部14内のタイトル鍵領域14aに記録されている。時変鍵抽出更新部15は最初のブロックB1の復号化の際に時変鍵1を抽出する。また時変鍵抽出更新部15は時点t1において、タイトル鍵領域14aに格納されているタイトル鍵を時変鍵1で上書き、すなわち書き換える。

【0049】次に記録用暗号化・復号化部12は時変鍵1を用いてブロックB2を復号化する。時変鍵抽出更新部15は2番目のブロックB2の復号化の際に時変鍵2を抽出し、時点t2において時変鍵1を時変鍵2で上書きする。以後、時変鍵3、時変鍵4...という手順で、時変鍵抽出更新部15はタイトル鍵領域14aの鍵を順次上書きしていく。

【0050】このようにブロック単位の復号化の際得られた時変鍵でタイトル鍵領域14aを順次上書きしていくことで、上書きした時変鍵を用いて復号化されるブロックより前のブロックの復号化が不可能となり、コンテンツそのものを削除した場合と同一の結果が得られる。

【0051】図13は本方式におけるコンテンツ削除方

式を適用した場合のMOVE処理において、処理中に障害が発生した場合の動作を示した図である。

【0052】図13では、ブロックB3を時変鍵Jk2で復号後、得られた時変鍵Jk3でタイトル鍵領域14aを上書きした後、障害が発生した場合を想定している。障害の具体例としては、停電による電源クラッシュや故障または不注意により伝送ケーブル抜き等が考えられる。この時すでに転送済みのコンテンツ（ブロックB1からB3）は消去済みもしくは2度と復号化できない状態であればならない。

【0053】本方式によるコンテンツ削除方法を適用したMOVE処理では、障害発生時点でタイトル鍵領域14aはJk3に書き換えられており、元のタイトル鍵Tkとそこから導出される時変鍵Jk1およびJk2は2度と得ることができない。このためブロックB1～B3のコンテンツは復号化不可能となり、事実上コンテンツが削除されたと同様の結果が得られる。

【0054】障害発生後、処理を再開する場合、タイトル鍵領域14aのJk3を用いてブロックB4を復号化し、該復号化の際に導出されるJk4を用いてブロックB5を復号化し、以後同様に残りのコンテンツを復号化して伝送することが出来る。

【0055】図14は本方式によるコンテンツ削除方式を用いたMOVE処理におけるタイトル鍵上書きのタイミングについて示した図である。

【0056】MOVE処理においては、前述したようにコンテンツの各ブロックの復号化時点で抽出された時変鍵を、タイトル鍵領域に順次上書きしていく。これにより、送信分のコンテンツ削除を保証できる。

【0057】図15は本方式によるコンテンツ削除方式を用いたPAUSE処理におけるタイトル鍵上書きのタイミングに関する第1の具体例について示した図である。

【0058】PAUSE処理においては記録時から制限時間（例えば90分）経過したコンテンツを順次削除していく必要がある。第1の具体例では、図中再生位置P1で示される再生のためのコンテンツ復号化とは別に、位置P2に示すように記録時から制限時間分前のコンテンツを並列に復号化処理し、当該復号化処理で得られた時変鍵をタイトル鍵領域14aに上書きする。尚、再生のためのコンテンツ復号化の際に得られる時変鍵は保存しない。

【0059】図16は本方式によるコンテンツ削除方式を用いたPAUSE処理におけるタイトル鍵上書きのタイミングに関する第2の具体例について示した図である。

【0060】第2の具体例ではタイムシフト再生の時点で得られた時変鍵をタイトル鍵記憶部14の一時保存領域14bに一時的に保存しておき、制限時間になった時点で順次上書きしていく。これは再生位置と制限時間の

間隔が短い場合やコンテンツ分割の間隔が大きい場合など記録すべき時変鍵の数が少ない場合に有効である。この時変鍵の一時保存領域14bはタイトル鍵領域14a同様、セキュアな領域に保護される必要がある。なお本実施形態では一時保存する時変鍵を制限時間までとしているが、インスタントリプレイが例えば数分など短時間であり、制限時間分再生位置に戻す必要がないなどの条件を満たせば、再生位置から例えば5分前まで保存するなど、保存する時変鍵の数を削減してもよく、時変鍵の保存期間は制限時間内で自由に設定できる。

【0061】図17は、本方式によるコンテンツ削除方式を用いたPAUSE処理におけるタイトル鍵上書きのタイミングに関する第3の具体例について示した図である。

【0062】第3の具体例ではタイムシフト再生の時点で得られた時変鍵を直接タイトル鍵領域に上書きする。これはコンテンツの一時停止のみをサポートし、インスタントプレイなど同一コンテンツを2度再生する必要が無い場合に有効である。

【0063】図18は本発明に係るコンテンツ削除の第2の実施形態を示した図である。

【0064】図18ではコンテンツ復号化の際得られた時変鍵を逐次タイトル鍵領域に上書きするのではなく、特定区間の復号化を完了するごとにタイトル鍵の上書きを行う。具体的にはMOVE処理やPAUSE処理で要求される最小消去単位や、表示や伝送の単位など意味のある復号化が可能な最小単位が、暗号化・復号化に用いるブロックより大きい場合に有効である。復号化特定区間の具体例としてはMPEGにおけるフレーム単位・GOP単位やMPEG2-TSにおけるPES単位、IEEE1394におけるIsochronous Streamパケット単位、特定の時間単位などがある。特定区間は固定長である必要は無く、あるルールに従い区間の特定が可能であればよい。これによりタイトル鍵の上書き回数が削減され処理の効率化が図れる。

【0065】図19は本実施形態によるコンテンツ復号化処理時におけるコンテンツ削除方法を示すフローチャートである。

【0066】ステップS01で記録用暗号化・復号化部12はタイトル鍵領域14aからタイトル鍵を取得する。ステップS02で暗号化コンテンツから1ブロック読み込む。ステップS03でタイトル鍵もしくは時変鍵を用いて1ブロックの暗号化コンテンツを復号化する。ステップS04で時変鍵抽出更新部15はステップS03の復号化により導出された新しい時変鍵を抽出する。ステップS05でコンテンツ削除要否判定部16は現在の処理がMOVE処理もしくはPSUSE処理であることを判定し、MOVE処理もしくはPAUSE処理であれば（コンテンツ削除の必要があれば）ステップS06へ進み、そうでない場合はステップS08に進む。ステ

ップS06で復号化区間判定部17は特定区間の復号化が完了したかどうかを判定し、完了していればステップS07へ、完了していなければステップS08へ進む。ステップS07で時変鍵抽出更新部15はタイトル鍵領域14aを新しい時変鍵で更新する。ステップS08でCPU18はコンテンツの全ブロックを復号化したか判定し、未復号化コンテンツが存在すればステップS02に戻って処理を継続し、全てのブロックを復号化していれば終了する。

【0067】図20は本方式に係るコンテンツ削除の別の具体例を示した図である。

【0068】図20では特定区間の最後のブロックの復号化の際、特定区間の最初のブロックの復号化の際に使用した時変鍵を使用する。つまり、特定区間の最初のブロックを例えば時変鍵jknを用いて復号化した場合、該特定区間の最後のブロックも時変鍵jknを用いて復号化する。このとき時変鍵jkn+1が抽出される。次の特定区間の最初のブロック及び最後のブロックは時変鍵jkn+1を用いて復号化する。従って、特定区間の最後のブロックの復号化の際、前ブロックの最後の復号化により抽出された時変鍵を用いる。これにより複数区間をまたがる場合の時変鍵の導出を高速に行うことができる。これは、特定倍速再生などの特殊再生や巻戻し後の再生の際効果がある。

【0069】なお本実施例では最後のブロックの復号化に最初のブロックの復号化に用いた時変鍵を適用した例を示したが、これは一般に後半のブロックの復号化の際に直前より前のブロックの復号化の際得られた時変鍵を適用すれば処理を効率化できる。ブロック復号化とそれに用いる時変鍵の組み合わせは本実施例の限りではない。

【0070】図21は図20で示したコンテンツ削除方式を用いた場合における特殊再生およびサーチの動作を示す図である。

【0071】図21(a)は倍速再生を示す図、図21(b)はサーチ動作を示す図である。倍速再生領域及びサーチ領域における斜線領域は1画像フレームを示す。又、斜線で示された領域は全ブロックを復号化した領域、空白領域は特定区間の最後のブロックのみを復号化した領域である。

【0072】通常の復号化処理では先頭からすべてのブロックを復号化しなければ特定位置の時変鍵は得られないが、図20に示すコンテンツ削除方式を用いた場合、特殊再生やサーチの際に時変鍵を再計算する場合でも、特定ブロックの最後のみ復号化すればよいため、高速に所定位置の時変鍵を得ることが出来る。

【0073】次に図22、図23を用いて、本発明を用いたコンテンツ削除方法に係る第3の実施形態について説明する。

【0074】図22は、従来におけるコンテンツ削除方

法に関する別の具体例を示す図である。

【0075】コンテンツを暗号化する際、コンテンツすべてを連続して暗号化するのではなく、特定の単位で処理を一旦リセットし、はじめから暗号化の処理を行う場合がある。例えばSD(Secure Digital)カードでは図22に示すように暗号化を音声フレーム単位に行う。このように各復号化の際に同一のタイトル鍵Tk1を用いるため、最終フレームを復号化完了するまでタイトル鍵Tk1を削除することができない。

【0076】図23は上記のような暗号化が適用された場合におけるコンテンツ削除方法に係る本発明の第3の実施形態を示した図である。

【0077】この例では、フレーム内の暗号化に用いる時変鍵とは別に、各フレームについても時変鍵を用いて暗号化する。これによりフレーム単位に暗号化を行う場合についても、MOVEやPAUSE時に本方式によるコンテンツ削除方式を適用することが出来る。

【0078】図24は本発明を用いたコンテンツ削除における鍵の更新方法の一具体例を示す図である。t0、t1…は各処理が行われた時点を示す。

【0079】タイトル鍵領域を時変鍵で更新する場合、時点t1のように直接上書きする代わりに一時領域に書き込みを行う。その後時点t3のように更新フラグを1に変更する。一時領域はタイトル鍵記憶部14内に設けられ、更新フラグはタイトル鍵記憶部14あるいは他の不揮発性メモリ領域に設けられる。次に、t4のようにタイトル鍵領域の鍵を更新し、更新終了後時点t6のように更新フラグを0に戻す。これにより鍵の更新中、障害によりクラッシュした場合、更新フラグが1の場合は一時領域の鍵、更新フラグが0の場合はタイトル鍵領域の鍵を参照することで、クラッシュによる鍵の消失を防ぐことができる。

【0080】

【発明の効果】以上説明したように本発明によれば、著作権保護機能により保護されたコンテンツをMOVE処理もしくはPAUSE処理する際に、元のコンテンツを安全かつ効率的に削除することができる。

【図面の簡単な説明】

【図1】本発明に係るコンテンツ管理装置の構成の一実施形態を示すブロック図。

【図2】コンテンツに付与される著作権保護情報の一例を示す図。

【図3】著作権保護のかかったコンテンツに対するMOVE・PAUSE処理の概要を示す図。

【図4】MOVE処理を具体的に説明する図。

【図5】PAUSE処理を具体的に説明する図。

【図6】従来におけるコンテンツを削除する第1の方式を示した図。

【図7】従来におけるコンテンツを削除する第2の方式を示した図。

【図8】従来におけるコンテンツを削除する第3の方式を示した図。

【図9】本方式におけるコンテンツを削除する方式の概略を示した図。

【図10】コンテンツ暗号化方式の一例を示す図。

【図11】図10で示した暗号化方式により暗号化されたコンテンツを復号化する処理を示した図。

【図12】本発明に係るコンテンツ復号化の際に行われるコンテンツ削除処理の第1の実施形態について示した図。

【図13】本方式におけるコンテンツ削除方式を適用した場合のMOVE処理において、処理中に障害が発生した場合の動作を示した図。

【図14】本方式によるコンテンツ削除方式を用いたMOVE処理におけるタイトル鍵書きのタイミングについて示した図。

【図15】本方式によるコンテンツ削除方式を用いたPAUSE処理におけるタイトル鍵書きのタイミングに関する第1の具体例について示した図。

【図16】本方式によるコンテンツ削除方式を用いたPAUSE処理におけるタイトル鍵書きのタイミングに関する第2の具体例について示した図。

【図17】本方式によるコンテンツ削除方式を用いたP

AUSE処理におけるタイトル鍵書きのタイミングに関する第3の具体例について示した図。

【図18】本発明によるコンテンツ削除の第2の実施形態を示した図。

【図19】本方式によるコンテンツ復号化処理時におけるコンテンツ削除方法を示すフローチャート。

【図20】本方式によるコンテンツ削除の別の具体例を示した図。

【図21】図20で示したコンテンツ削除方式を用いた場合における特殊再生およびサーチの動作を示す図。

【図22】従来におけるコンテンツ削除方法に関する別の具体例を示す図。

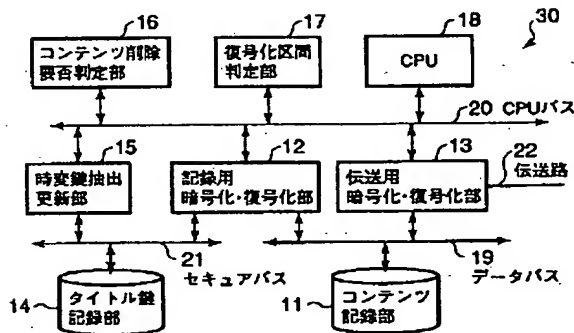
【図23】図22のような暗号化が適用された場合におけるコンテンツ削除方法に係る本発明の第3の実施形態を示す図。

【図24】本発明を用いたコンテンツ削除における鍵の更新方法の一具体例を示す図。

【符号の説明】

11…コンテンツ記録部、12…記録用暗号化・復号化部、13…伝送用暗号化・復号化部、14…タイトル鍵記録部、15…時変鍵抽出更新部、16…コンテンツ削除要否判定部、17…復号化区間判定部、18…CPU、19…データベース、20…CPUバス、21…セキュアバス、22…伝送路、30…コンテンツ管理装置

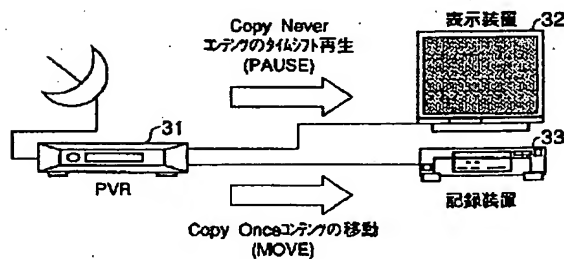
【図1】



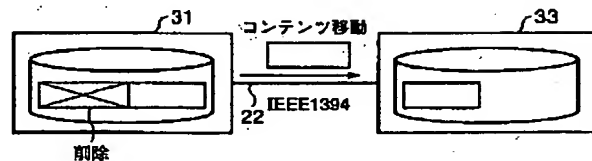
【図2】

データ	定義
00	Copy Free
01	No More Copy
10	Copy Once
11	Copy Never

【図3】



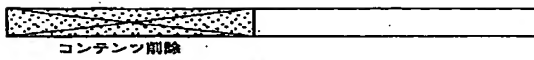
【図4】



【図5】



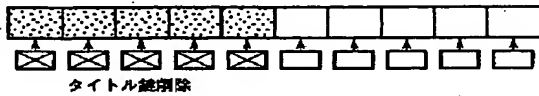
【図6】



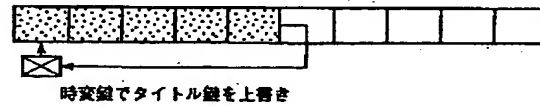
【図7】



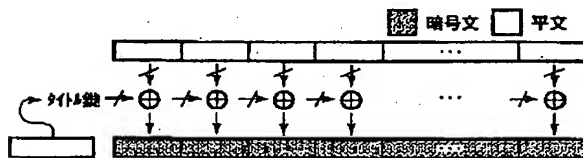
【図8】



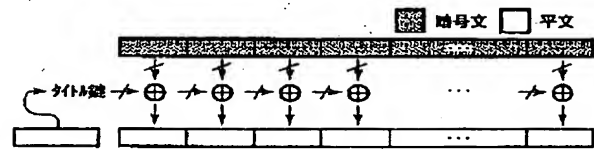
【図9】



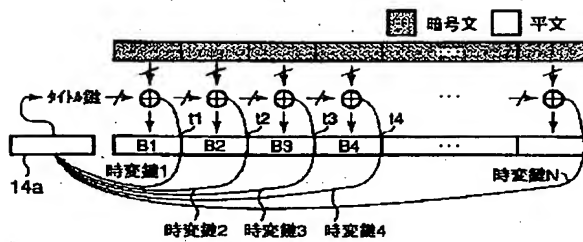
【図10】



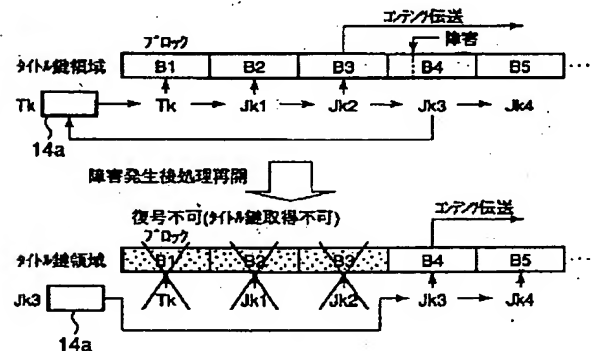
【図11】



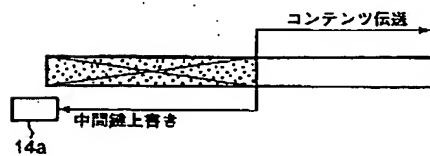
【図12】



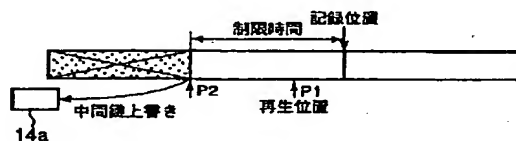
【図13】



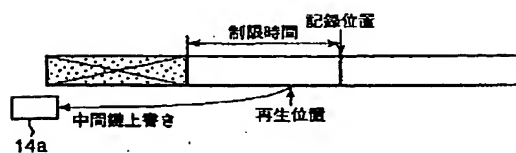
【図14】



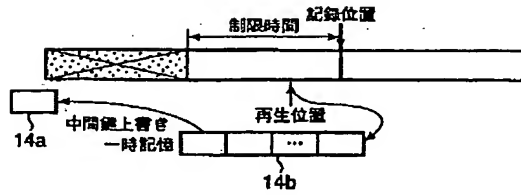
【図15】



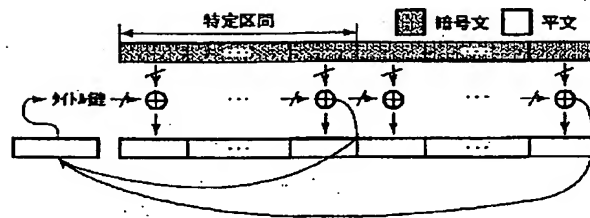
【図17】



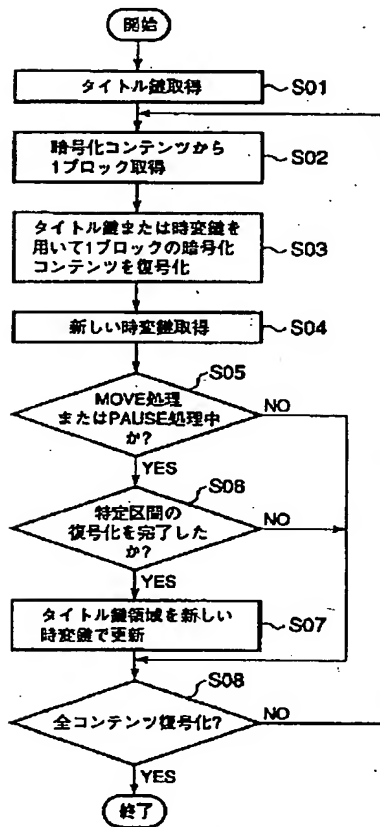
【図16】



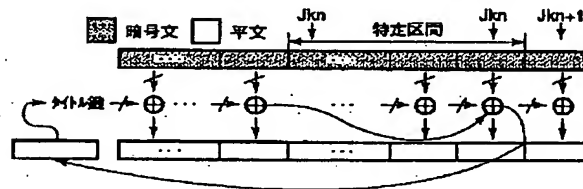
【図18】



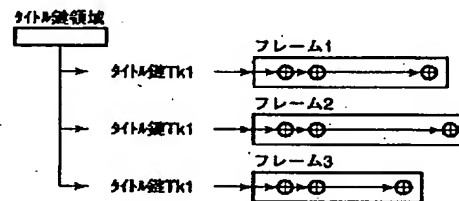
【図19】



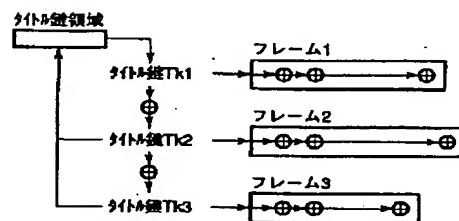
【図20】



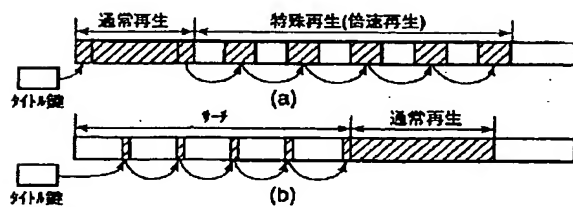
【図22】



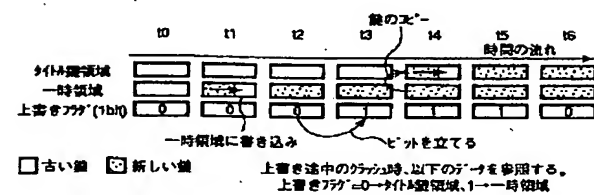
【図23】



【図21】



【図24】



フロントページの続き

(51) Int. Cl. 7	識別記号	F I	ターム (参考)
H O 4 N	5/765	H O 4 L 9/00	6 4 3 5 D 0 4 4
	5/91	H O 4 N 5/91	P 5 J 1 0 4
	5/92		L
	5/93	5/92	H
	7/08	5/93	E
	7/081	7/08	Z
	7/167	7/167	Z
	7/173		

6 3 0

F ターム (参考) 5B017 AA07 BA07 CA16
 5C052 AA01 AB03 AC05 CC06 CC11
 DD04
 5C053 FA13 FA20 FA21 FA23 GA11
 GB06 GB37 HA24 JA21 KA24
 LA06 LA07 LA15
 5C063 AA01 AB03 AB05 AC01 AC05
 AC10 CA11 CA23 CA36 DA07
 DA13 DB10
 5C064 BA01 BB02 BC06 BC17 BC18
 BC22 BC23 BC25 BD02 BD08
 BD09 BD13 CA14 CB01 CC04
 5D044 AB05 AB07 BC01 BC04 CC04
 DE17 DE50 EF05 FG18 GK17
 HL08
 5J104 AA01 AA34 NA02